Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Information Technology

Unit 11: Cyber Security and Incident Management

Part A

Window for supervised period:
Monday 30 April 2018 – Monday 21 May 2018
Supervised hours: 5 hours

Paper Reference
20158K

You must have:
Risk_Assessment.rtf
Security_Plan.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this task is 43.

Turn over ▶

P57172A

©2018 Pearson Education Ltd.

1/1/1/1/1/1

P 5 7 1 7 2 A

Pearson

Instructions to Teachers/Tutors and/or Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of three weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for candidate use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Teachers/tutors may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Teachers/tutors and invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 25 May 2018.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your teacher/tutor may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within your folder, using the file names listed.

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your teacher/tutor.

BLANK PAGE

Set Task Brief

Black Country Training and Assessment

Black Country Training and Assessment (BCTAA) offers vocational-based training and assessment services for small and medium-sized businesses.

Some training is routine, such as running food safety or IT skills courses. It uses a database of freelance trainers and assessors to meet client requirements.

BCTAA also develops bespoke training and assessment for specialised skills, such as the maintenance of unusual machinery or working with a unique production process. Bespoke training requires collaboration with the client and often includes handling highly confidential information, such as trade secrets.

Full-time Training Managers meet clients and work with them to create and run bespoke training and assessment.

BCTAA is moving from a business park on the outskirts of Birmingham to a larger city centre premises. The company has taken a lease on the 19th floor of a 20 storey building, Edexcelsior House (EH).

EH has mixed commercial and office usage. The 18th floor is leased by a recruitment agency. There is a restaurant and coffee bar on the 20th floor and a bar-cafe in the garden on the roof. There are several small retail units on the ground floor. There is a gym, an art gallery and meeting rooms on other floors. A number of different companies have office space in the building.

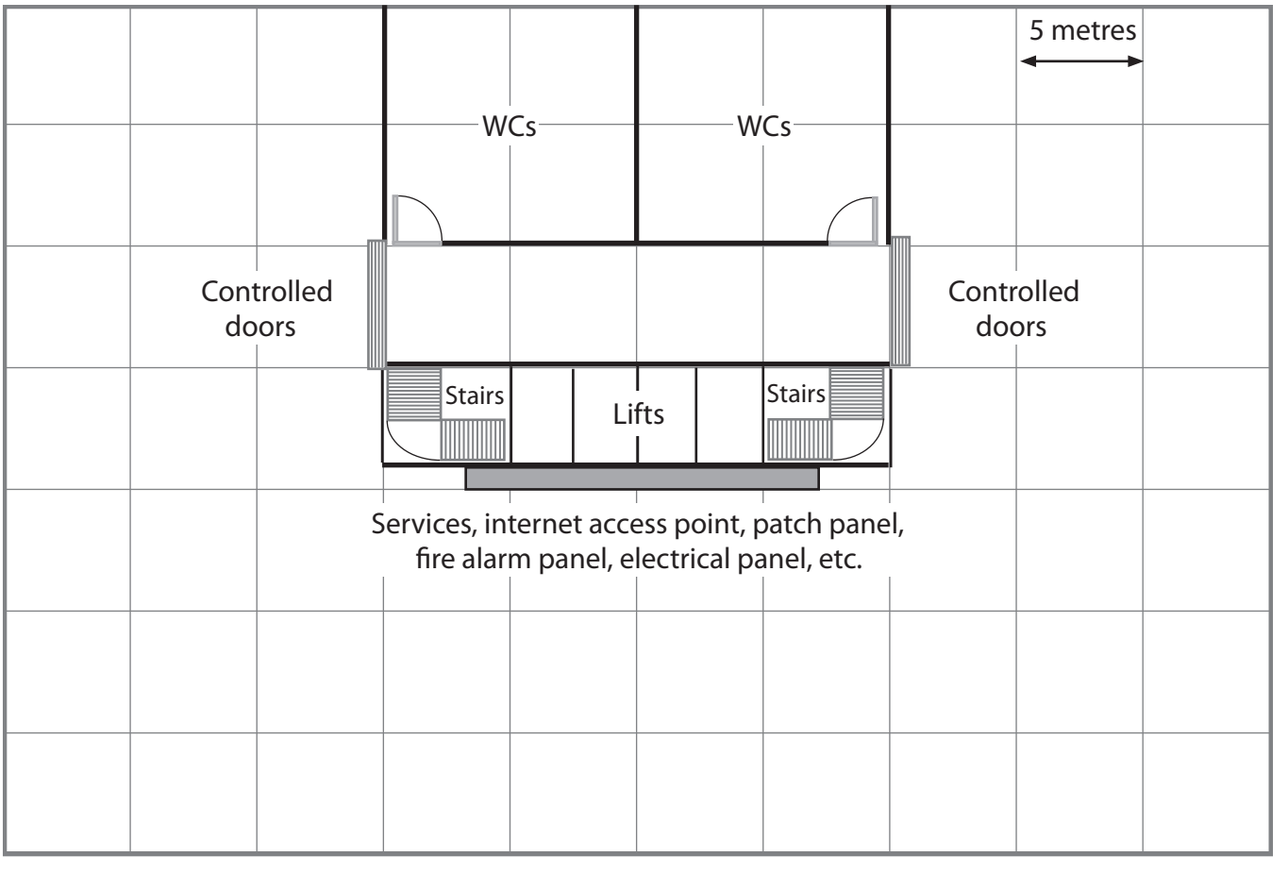

Figure 1

A plan of the 19th floor, to be leased by BCTAA, is shown in **Figure 1**.

Most of the public areas are open outside of normal office hours and the restaurant and bar are popular in the evening.

The lifts, stairs, WCs and all the area around them are used by the public. The remaining area is a single open space that can be partitioned to create rooms or workspaces.

The 19th floor has many electrical points. The data outlets have an optical fibre internet access point. The data outlets are connected by Cat6 cable to a patch panel near the internet access point. BCTAA will have to setup their own network devices.

The private areas of the 19th floor are protected by a card reader door control system. This uses near field communication/proximity cards, similar to those used for contactless payment systems. The readers are already in place for each door. The EH management company supplies cards, a card programming device and logging and control software. The doors can also be unlocked from the inside by means of a push button.

BCTAA has asked you to advise on setting up and securing its network in its new location. Your contact is Baljinder Singh an experienced computer user who is responsible for the current network. He is not a network specialist and says that the current system "had stuff added when we thought it was needed". Baljinder has produced the basic network design, but wants you to review his ideas and make sure the new system is secure from the start.

Figure 2 shows the outline network diagram received from Baljinder.

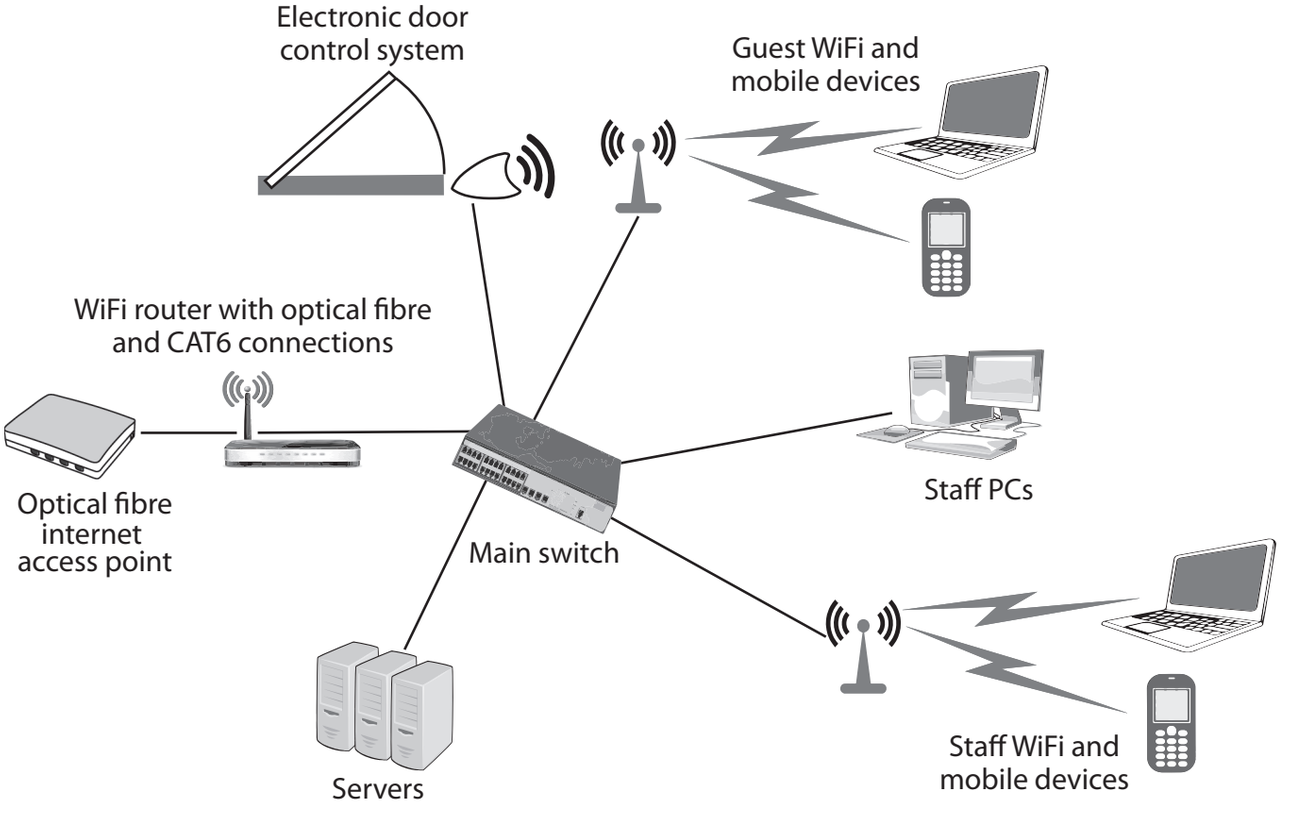

Figure 2

Development plan

At a meeting with Baljinder, you agree these points on the development of the new BCTAA network.

1. The network will conform to the outline network diagram.
2. The network uses private, Class C, IPv4 addresses.
3. The Edexcelsior internet access system will be kept and will use a fibre optic connection point.
4. The door control system will not be changed.
5. The BCTAA network must be protected against intrusion through the internet.
6. The router must include a firewall and relevant cyber security technology to protect the network.
7. Both staff and visitors must be able to connect using mobile devices.
8. Some visitors will be clients who may need access to appropriate secure areas of the network.
9. Freelance trainers and assessors will need access to appropriate secure areas of the network from home or work locations.
10. Some staff will need access to secure areas from home or client company locations.
11. A virtual private network (VPN) will be used to facilitate items 9 and 10.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

Baljinder is aware that the BCTAA network is vulnerable to attack. You have been hired to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan _[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS
TOTAL FOR PART A = 43 MARKS

BLANK PAGE

BLANK PAGE